IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Jamal Benbrahim	Attorney Docket No.: IGT1P376/P-227
Application No.: 09/880,474	Examiner: Emmanuel Omotosho
Filed: June 12, 2001	Group: 3714
Title: METHOD AND APPARATUS FOR SECURING GAMING MACHINE OPERATING DATA	Confirmation No.: 5212

CERTIFICATE OF EFS-WEB TRANSMISSION
I hereby certify that this correspondence is being transmitted electronically through EFS-WEB to the Commissioner for Patents, P.O. Box 1450 Alexandria, VA 22313-1450 on June 23, 2008.
Signed: /swx/
Susan W. Xu

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a Notice of Appeal.

The review is requested for the reasons stated below.

SUMMARY OF THE CLAIMED INVENTION

Aspects of the invention relate to gaming machines and gaming operations.

As noted in the background section, gaming machines can be effectively controlled by gaming control code (or executable code) and data. Securing the control code and data used to effectively operate a gaming machine is crucial partly because serious consequences can result from even minor defects in the executable code or data. The executable code or data can also be subject to malicious attacks as certain individuals may attempt to temper with the control code and/or data in order to wrongfully gain large amounts of money.

Generally, the executable code and data used by gaming machines to conduct gaming operations should be secured. On the other hand, it is desirable to allow gaming machines to operate different games and/or receive executable code and/or data from various sources.

As noted in the background section, "...so that different games may be played on a particular machine or various features of the machine can be updated, in many instances the gaming machine is arranged to accept new control code or other data."

It will be appreciated that the invention, among other things, can provide techniques for receiving multiple gaming control code and data from remote devices, and securing storing and executing executable code and data on gaming machines (see, for example, Summary of the invention).

In accordance with one aspect of the invention, the claimed invention can utilize a novel combination of encryption and authentication techniques to allow reception of multiple games from a remote device, and securely executing the games on a gaming machine. In one embodiment, encrypted executable code and private keys are received by a gaming machine from a remote device (e.g., a first gaming server). After decrypting the encrypted executable code and successfully authenticating the decrypted code with a remote device (e.g., the first gaming server or a second gaming server designated for authentication), the gaming machine can execute the decrypted executable code and data (see, for example, claim 18).

As a representative claim, claim 18 pertains to method of operating a gaming device.

In brief, claim 18, recites:

(a) receiving from a remote device encrypted executable code for a plurality of games including a first game and a second game, wherein the first game includes a first set of operating data encrypted with a first private key, and the second game includes a second set of operating data encrypted with a second private key;

(b) storing on the gaming device the encrypted executable code for both the first game and second game;

(c) receiving by the gaming device from the remote device only one of the first private key or the second private key in order to prevent execution of the first game or the second game on the gaming device;

(d) decrypting, by the gaming device, one of the first set of operating data or the second set of operating data according to the one of the first private key or the second private key selected to recover the one of the first set of operating data or the second set of operating data;

(e) sending, by the gaming device, information relating to the decrypted one of the first set of operating data or the second set of operating data to a remote device for authentication of the decrypted one of the first set of operating data or the second set of operating data after decrypting one of the first set operating data or the second set of operating data;

(f) taking remedial action by the gaming device when the decrypted one of first set of operating data or the second set of operating data is not authenticated by the remote device, wherein the remedial action includes not allowing the decrypted one of first set of operating data or the second set of operating data to be executed by the gaming device;

(g) storing the decrypted one of the first set of operating data or the second set of operating data on the gaming device when the decrypted one is authenticated by the remote device; and

(h) executing the first game or the second game on the gaming device utilizing the decrypted one of the first set of operating data or the second set of operating data when the decrypted one is authenticated by the remote device.

THE EXAMINER'S REJECTION OF THE CLAIMED INVENTION

In the Final Office Action, the Examiner has rejected claims 18-40 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,645,077 (*Rowe*) in view of U.S. Patent No. 5,991,399 (*Graunke et al.*) and Patent No. 6,149,522 (*Alcorn et al.*). The Finality and substance of the Examiner's rejection is traversed below for at least the following reasons:

(i) THE FINALITY OF THE REJECTION IS IMPROPER BECAUSE THE EXAMINER HAS NOT ADDRESSED ALL OF THE CLAIMED FEATURES

Claim 18, among other things, recites*: (A) receiving from a remote device encrypted executable code for a plurality of games, and (B) storing the encrypted executable code on a gaming device.*

Initially, it is respectfully submitted that the Examiner has not addressed these claimed features (A and B) in the Final Office Action. Accordingly, it is respectfully that the Finality of the rejection is improper and should be withdrawn for at least these reasons.

Moreover, it is earnestly believed that the cited art does not teach or suggest these claimed features and claim 18 is therefore patentable over the cited art at least for this reason.

(ii) THE CITED ART DOES NOT TEACH OR SUGGEST: (C) RECEIVING BY A GAMING DEVICE ONLY ONE OF A FIRST PRIVATE KEY OR A SECOND PRIVATE KEY FOR RESPECTIVELY DECRYPTING ENCRYPTED FIRST AND SECOND OPERATING DATA WHICH ARE STORED ON A GAMING DEVICE FOR FIRST AND SECOND GAMES IN ORDER TO PREVENT THE EXECUTION OF THE FIRST OR SECOND GAME ON THE GAMING DEVICE (CLAIM 18)

It should be noted that receiving only one of the first or second private keys can effectively prevent the execution of the first or second game on the gaming machine.

It is respectfully submitted that the Examiner has not properly addressed this claimed feature in the Final Office Action. Instead, the Examiner has merely asserted that *Graunke et al.* teaches "...utilize[ing] private key for cryptographic processing data," and "...taking remedial action whenever the decrypted data is not authenticated by the remote device" (Final Office Action, page 3).

Clearly, this general assertion does not address the specific claimed feature of: *receiving by a gaming device only one of a first private key or a second private key for respectively decrypting encrypted first and second operating data which are stored on a gaming device for first and second games, in order to prevent the executing of the first or second game on the gaming device*.

In the Final Office Action, the Examiner has also asserted that "the only way to prevent an individual from accessing encrypted data is not to provide the individual the key to decrypt the encrypted data," and as such, the claimed feature would have been well known (Final Office Action, page 7).

Contrary to the Examiner's assertion, it is respectfully submitted that there are other mechanisms for preventing an individual from accessing encrypted data. For example, an individual may not be provided with the encrypted data and/or not be granted permission to access the encrypted data in the first place. As such, it is very respectfully submitted that the Examiner's assertion is improper.

Furthermore, it is respectfully submitted that the Examiner needs to provide factual evidence to show that a specific claimed feature is taught by the prior art rather than make a general allegation without providing any factual evidence to show how that the specific claimed feature can possibly be taught by the general principals of encryption. Clearly, the Applicant has not over broadly claimed encrypting and decrypting data. As such, it is respectfully submitted that the Examiner's rejection is improper for failing to properly address this specific claimed feature (C).

Moreover, it is earnestly believed that the cited art does not teach or suggest this claimed features and claim 18 is therefore patentable over the cited art for this additional reason.

(iii) THE OFFICE ACTIONS FAIL TO INDICATE HOW THE CITED ART TEACHES OR SUGGESTS: (D) SENDING BY A GAMING DEVICE INFORMATION RELATED TO A DECRYPTED ONE OF FIRST OR SECOND OPERATING DATA FOR AUTHENTICATION AFTER DECRYPTING IT RESPECTIVELY BY THE FIRST OR SECOND PRIVATE KEY (CLAIM 18)

In the Final Office Action, the Examiner has asserted that *Alcorn et al.* teaches the claimed feature of: sending, by a gaming device, information related to the decrypted one of the first or second operating data (for first and second games) for authentication after decrypting it respectively by the first or second private key (Final Office Action, page 4).

The Examiner has not explained how the abstract of *Alcorn et al.*, considered alone or in view of the general knowledge that a message digest can be determined, or authentication in the broad sense, do not address this specific claimed feature (D). Accordingly, it is respectfully submitted that the Examiner's rejection is improper and should be withdrawn for this additional reason.

Moreover, it is earnestly believed that the cited art does not teach or suggest this claimed features and claim 18 is therefore patentable over the cited art for yet an additional reason.

(iv) THE EXAMINER HAS FAILED TO ESTABLISH A PRIMA FACIE CASE OF OBVIOUSNESS

It is respectfully submitted that the Examiner has failed to establish a prima facie case of obviousness because the Examiner has failed to provide any factual evidence to show that the combination of *Rowe, Graunke et al., and Alcorn et al.* teach all the specific claimed features, or the combination of the specific claimed features would have been obvious in the first place.

Instead, the Examiner has merely asserted that "one of ordinary skill in the art would have been forced to seek outside references, such as the *Graunke et al.* reference for disclosure as to the known manners and/or procedures of enacting the encryption as described in the first invention of Rowe" (Final Office Action, page 4), and *Alcorn et al.* teaches "a step of taking the security measures a step further to prevent tampering with the contents of the game data" (Final Office Action, page 5).

It is very respectfully submitted that these general allegations do not provide the factual evidence needed to support a prima facie case of obviousness.

(v) THE CITED ART DOES NOT TEACH THE COMBINATION OF THE CLAIMED FEATURES

Moreover, it is respectfully submitted that the cited art cannot possibly teach or suggest the combination of the claimed features recited in claim 18 (a, b, c, d, e, f, g and h) and claim 18 is therefore patentable over the cited art. Other independent claims recite similar features as those discussed above and are believed to be patentable over the cited art for at least the same reasons.

I am the attorney or agent acting under 37 CFR 1.34.

Respectfully submitted,
BEYER LAW GROUP LLP

/RMahboubian/
Ramin Mahboubian
Reg. No. 44,890

P.O. Box 1687
Cupertino, CA 95015-1687
408-255-8001